⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−15886

⑤Int.Cl.'	識別記号	庁内整理番号
G 09 C 1/00		7343−5B
G 06 F 7/552	A	7056−5B
7/72		7056−5B

⑬公開　平成3年(1991)1月24日

審査請求　未請求　請求項の数 2　(全6頁)

⑤④発明の名称　べき乗剰余計算装置

②①特　願　平1−149397

②②出　願　平1(1989)6月14日

⑦②発明者　髙林　京子　神奈川県川崎市幸区小向東芝町1　株式会社東芝総合研究所内

⑦①出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地

⑦④代理人　弁理士　三好　秀和　外1名

明　細　書

1．発明の名称

べき乗剰余計算装置

2．特許請求の範囲

(1)　P，C，Dが入力データで、べき乗剰余計算 $C^D \bmod P$ を計算するべき乗剰余計算装置において、

D′＝(P−1)−Dで表わされるD′を計算する手段と、DもしくはD′を指数としたときの乗算回数Td又はTd′を計算する手段と、CとPが互いに素で前記乗算回数がTd＞Td′のときには $C^{D'} \bmod P$ の乗法的逆元を出力し、それ以外のときには $C^D \bmod P$ を出力する手段とを具備することを特徴とするべき乗剰余計算装置。

(2)　前記乗算回数を計算する手段は、指数Xを2進展開したときのXの桁数及び‘1’の数から乗算回数を計算することを特徴とする請求項1に記載のべき乗剰余計算装置。

3．発明の詳細な説明

［発明の目的］

（産業上の利用分野）

本発明は、処理桁数の大きなべき乗剰余計算に好適なべき乗剰余計算装置に関するものである。

（従来の技術）

公開鍵暗号方式の中で最も注目されているRSA暗号の復号化は、次式で示されるように、べき乗剰余計算を行って暗号文Cから平文Mを復号することにより以下のように行なわれる。

$$M = C^D \bmod N$$

ただし、M：平文

C：暗号文

D：秘密鍵

N：2つの素数P，Qの積

従来のRSA暗号の復号化方式としては、「RSA暗号の復号化装置」（特開昭63−129388）が知られている。

第4図は、この方式を説明するためのフローチャートである。この方式ではまず、入力データC，法N(＝PQ)，指数D，法Nとの最大公約数gcd(C，N)が1かどうかを示すフラグFLGを

初期設定する（ステップ４０１）。

次に、ステップ４０２でフラグＦＬＧが"１"であると判別された場合には、指数Ｄ′（＝（Ｐ－１）（Ｑ－１）－Ｄ）を用いてべき乗余剰の計算を行った後（ステップ４０３）、その結果Ｍ′の乗法的逆元Ｍ″を計算して、入力データＣの復号結果とする（ステップ４０４）。

一方、ステップ４０２でフラグＦＬＧが"１"以外の値であると判別された時は、指数Ｄを用いてべき乗剰余の計算をし、その結果を復号結果とする（ステップ４０５）。

この方式では、Ｄ′のとる範囲がＤと同じ０＜Ｄ′＜Ｎで、ｇｃｄ（Ｃ，Ｎ）＝１の時は常にＤ′で計算するので、Ｄによってはかえって計算量が増加してしまうという問題があった。

（発明が解決しようとする課題）

以上述べたように、従来の方式はＤ′を用いてべき乗剰余計算をすると、Ｄで計算するよりも計算量が増加してしまう場合があるという欠点があった。

従って、本発明ではＤを用いてべき剰余計算をするよりも常に計算量が少なくなるべき乗剰余計算装置を提供することを目的とする。

〔発明の構成〕

（課題を解決するための手段）

この発明は、上記の目的を達成するために、Ｐ，Ｃ，Ｄが入力データで、べき乗剰余計算 $C^D \bmod P$ を計算するべき乗剰余計算装置において、Ｄ′＝（Ｐ－１）－Ｄで表わされるＤ′を計算する手段と、ＤもしくはＤ′を指数としたときの乗算回数Ｔｄ又はＴｄ′を計算する手段と、ＣとＰが互いに素で前記乗算回数がＴｄ＞Ｔｄ′のときには $C^{D'} \bmod P$ の乗法的逆元を出力し、それ以外のときには $C^D \bmod P$ を出力する手段とを具備することを特徴とするものである。

特に、前記乗算回数を計算する手段としては、指数Ｘを２進展開したときのＸの桁数及び"１"の数から乗算回数を計算するものが好ましい。

（作用）

本発明によれば、指数計算を素数Ｐのもとで計算する場合、指数ＤからＤ′（＝（Ｐ－１）－Ｄ）を計算し、ＤとＤ′で計算量が少なくなる値を指数としてべき乗剰余計算を行うため、乗除算回数が減少し、高速にべき乗剰余計算を行うことができる。

更に、本発明とＱuisquater の方法を用いて、ＲＳＡ暗号の復号化処理を行う場合、本発明を組み合わせることにより、更に処理を高速に行うことができる。

（実施例）

以下、図面を参照して本発明の実施例を説明する。

具体的実施例の説明に入る前に、本発明の原理を以下に述べる。

$C^D \bmod P$ を計算する場合、ＣとＰが互いに素の時は、Ｄ′（＝（Ｐ－１）－Ｄ）をＤの変わりに指数として用いてべき乗剰余計算をおこなっても同じ結果となる。これはフェルマーの小定理から導くことができる。

フェルマーの小定理とは、

『ｐが素数ならば、ｇｃｄ（ａ，ｐ）＝１なるａに対して、常に

$$a^{P-1} \equiv (\bmod\ p)$$

が成立する。』

である。

よって、Ｄ′を指数としてフェルマーの小定理を用いると

$$M' = C^{D'} \bmod P$$

$$= C^{(P-1)-D} \bmod P$$

$$= \frac{C^{P-1} \bmod P}{C^D \bmod P} \bmod P$$

$$= \frac{1}{C^D \bmod P} \bmod P$$

続いて、Ｍ′の乗法的逆元Ｍを求めて復号結果とする。乗法的逆元を求めるには、拡張ユークリッドの互除法を用いれば良い。

法Ｐは素数なので、０＜Ｃ＜Ｐならば、入力データＣと法Ｐは必ず互いに素となり、すべての入力データＣに対して、本発明を適用することができる。

第１図は、第１の実施例における法を素数としたべき乗剰余計算装置の概要を示すブロック図である。

同図において、１０１は素数Ｐをセットするレジスタ、１０２は被べき乗数をセットするレジスタ、１０３は指数Ｄをセットするレジスタ、１１２は指数Ｄ′（＝（Ｐ－１）－Ｄ）を計算する回路、１０４は指数Ｄ′をセットするレジスタである。

また、１０５は指数Ｄのときの乗除算回数Ｔｄと指数Ｄ′のときの乗除算回数Ｔｄ′を計算する回路、１０６は法と被べき乗数が互いに素でＴｄ＞Ｔｄ′であるときフラグ"１"を立てておくフラグレジスタである。

また、１０７はフラグレジスタに"１"が立っている場合にはレジスタ１０４の出力を選択し、"１"が立っていない場合にはレジスタ１０３の出力を選択するマルチプレクサである。

１０８は前記レジスタ１０１の出力値Ｐと前記レジスタ１０２の出力値Ｃと前記マルチプレクサ１０７の出力値ＤまたはＤ′を入力として$C^{X} \bmod P$（Ｘ＝Ｄは又は、Ｄ′）を計算するべき乗剰余計算回路である。

１０９は前記フラグレジスタ１０６の値が"１"の時に前記べき乗剰余計算回路の出力値を後述する乗法的逆元計算回路側に出力し、それ以外の時は復号化出力側に出力するデマルチプレクサである。

また、１１０は前記フラグレジスタ１０６の値が"１"の時に、前記デマルチプレクサ１０９の出力値Ｍ′と前記レジスタ１０１の出力値Ｐを入力として、Ｍ′Ｍ″≡１ mod Ｐとなる Ｍ″を計算する乗法的逆元計算回路、１１１はべき乗剰余計算装置全体を制御する制御回路である。

第２図は、第１の実施例の処理手順を示すフローチャートである。まず、入力データＣ，法Ｐ，指数Ｄ，指数Ｄ′，フラグを初期設定する（ステップ２０１）。

次に、フラグ１の場合には（ステップ２０ＹＥＳ）、指数Ｄ′を用いたべき乗剰余の計算を行った後（ステップ２０３）、その出力値Ｍ′の乗法的逆元Ｍ″の計算を実行して、このＭ″を復号結果とする（ステップ２０４）

一方、フラグが１でない時は（ステップ２０２ＮＯ）、指数Ｄを用いてべき乗剰余の計算を実行し、その出力値Ｍを復号結果とする（ステップ２０５）。

但し、Ｄ′＝（Ｐ－１）－Ｄ

フラグＦＬＧ＝"０"…指数Ｄの乗除算回数＜指数Ｄ′の乗除算回数

フラグＦＬＧ＝"１"…指数Ｄの乗除算回数＞指数Ｄ′の常除算回数かつ、gcd（Ｃ，Ｐ）＝１

次に、本発明の第２の実施例について説明する。これは、本発明をＲＳＡ暗号の復号処理に利用しようというものである。本発明とQuisquaterの方法を用いた復号アルゴリズムを以下に述べる。

Quisquaterの方法は公開鍵Ｎの素因数ＰとＱを直接用いて復号処理を並列に計算する方法である。復号処理を行う人は秘密鍵Ｄを知っているので、秘密の素因数ＰとＱを直接用いても安全性は低下しない。ＲＳＡ暗号では、次式が成立する。

$$M = C^{D} \bmod N$$

$$N = PQ$$

ここでｃ１，ｃ２，ｄ１，ｄ２，ａ１，ａ２を、

$$c1 = C \bmod P$$

$$c2 = C \bmod Q$$

$$d1 = D \bmod P-1$$

$$d2 = D \bmod Q-1$$

$$a1 = M \bmod P$$

$$a2 = M \bmod Q$$

と定義すると、次式が成立することは明らかである。

$$a1 = c1^{d1} \bmod p$$

$$a2 = c2^{d2} \bmod q$$

ａ１，ａ２が求まれば、

$$M \equiv a1 \pmod p$$

$$M \equiv a2 \pmod q$$

なので、中国剰余定理により連立合同式を解いてＭが求まる。

次に、この方式と本発明を用いた高速復号法を説明する。

この方式に更に本発明を用いて、d 1′, d 2′を

$$d1' = (P-1) - d \bmod (p-1)$$

$$d2' = (Q-1) - d \bmod (q-1)$$

$$\alpha 1' = M^{d1'} \bmod p$$

$$\alpha 2' = M^{d2'} \bmod q$$

と定義する。

次に、被乗数をc 1、指数をd 1としたときの乗除算回数Td 1、被乗数をc 1、指数をd 1′としたときの乗除算回数Td 1′、被乗数をc 2、指数をd 2としたときの乗除算回数Td 2、被乗数をc 2、指数をd 2′としたときの乗除算回数Td 2′を計算する。

Td 1 > Td 1′のときはd 1′を指数として、それ以外の時はd 1を指数として用いて、べき乗剰余計算をする。Td 2, Td 2′についても同様である。

もしd 1′又はd 2′を用いてべき乗剰余計算を行った場合は、α 1′又はα 2′の乗法的逆元α 1′又はα 2′を計算する。

次に、中国剰余定理を用いて

$$M = x \pmod P \quad (x = \alpha 1 \text{又は} \alpha 1')$$

$$M = y \pmod Q \quad (y = \alpha 2 \text{又は} \alpha 2')$$

を解いてMを求めることができる。

第3図は、第2の実施例を示すブロック図である。同図において、301は指数Dをセットするレジスタ、302は素数Pをセットするレジスタ、303は素数Qをセットするレジスタ、304は被べき乗数Cをセットするレジスタである。

305は指数d 1 (= D mod P − 1)、指数d 1′ (= (P − 1) − D mod P − 1) 指数d 2 (= D mod Q − 1)、指数d 2′ (= (Q − 1) − D mod Q − 1) を計算する回路、306は前記d 1, d 1′, d 2, d 2′計算回路305からの出力を後述のレジスタ309, 310, 311, 312へ切替えるマルチプレクサである。

309は指数d 1をセットするレジスタ、310は指数d 1′をセットするレジスタ、311は指数d 2をセットするレジスタ、312は指数d 2′をセットするレジスタである。

307は指数d 1, d 1′, d 2, d 2′の2進展開したときの桁数と"1"の数から乗除算回数を計算する回路、308は法Qと被べき乗数c 2とが互いに素でTd 2 > Td 2′である時フラグ"1"を立てておくフラグレジスタである。

324は法Pと被べき乗数c 1とが互いに素でTd 1 > Td 1′である時フラグ"1"を立てておくフラグレジスタである。

313は前記レジスタ309, 310からの出力を前記フラグレジスタ324の値に応じた切替えるマルチプレクサ、314前記レジスタ311, 312からの出力を前記フラグレジスタ308の値に応じて切替えるマルチプレクサである。

315は前記レジスタ302の出力値Pと前記レジスタ304の出力値Cと前記マルチプレクサ313の出力値d 1又はd 1′を入力として、計算するべき乗剰余計算回路である。

316は前記レジスタ303の出力値Qと前記レジスタ304の出力値Cと前記マルチプレクサ314の出力値d 2又はd 2′を入力として計算するべき乗剰保計算回路である。

317は前記べき乗剰余計算回路315からの出力を前記フラグレジスタ324に"1"がたっていたら後述する乗法的逆元計算回路319に出力し、それ以外は後述するマルチプレクサ321に出力するデマルチプレクサである。

318は前記べき乗剰余計算回路316からの出力を前記フラグレジスタ308に"1"がたっていたら後述する乗法的逆元計算回路320に出力し、それ以外は後述するマルチプレクサ322に出力するデマルチプレクサである。

319は前記デマルチプレクサ317の出力値α 1′と前記レジスタ302の出力値Pを入力として、α 1′α 1′ ≡ 1 mod Pとなるα 1′を計算する乗法的逆元計算回路である。

320は前記デマルチプレクサ318の出力値α 2′と前記レジスタ303の出力値Qを入力と

して、■2′■2′≡1■od Qとなる■2′を計算する乗法的逆元計算回路である。

３２１は前記フラグレジスタ３２４に‘1’がたっている場合は前記乗法的逆元３１９の計算回路からの出力に切替え、それ以外の場合は前記デマルチプレクサ３１７からの出力に切替えるデマルチプレクサである。

３２２は前記フラグレジスタ３０８に‘1’がたっている場合は前記乗法的逆元の計算回路３２０からの出力に切替え、それ以外の場合は前記デマルチプレクサ３１８からの出力に切替えるデマルチプレクサである。

３２３は前記マルチプレクサ３２１，３２２からの出力から復号結果Ｍを求める中国剰余定理計算回路である。

［発明の効果］

以上説明したように、本発明によれば、素数Ｐを法としたべき乗剰余計算において、指数Ｄのかわりに Ｄ′（＝（Ｐ－１）－ｄ）を指数としてべき乗剰余計算を行う場合、べき乗剰余計算の乗除算回数が常に減少し、とくにQuisquaterの方式を使ってＲＳＡ暗号の復号化処理をする場合、本方式を組合わせて用いることにより更に高速に復号処理を行うことができる。

４．図面の簡単な説明

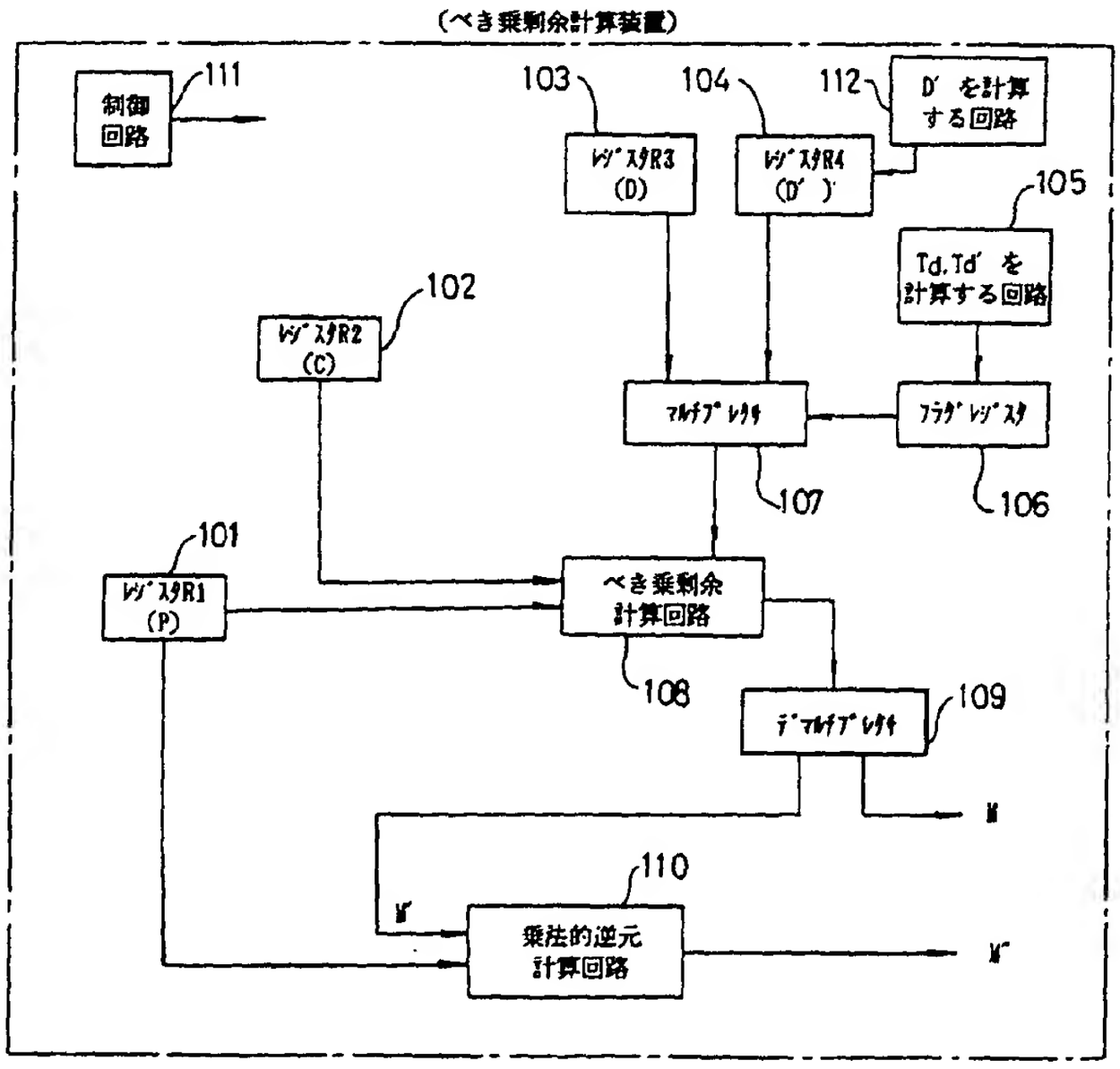
第１図は、本発明における第１の実施例のブロック図、第２図は同実施例の処理手順を示すフローチャート、第３図は第２の実施例のブロック図、第４図は従来のＲＳＡ暗号の復号装置のべき乗剰余計算のフローチャートである。

１０８…べき乗剰余計算回路

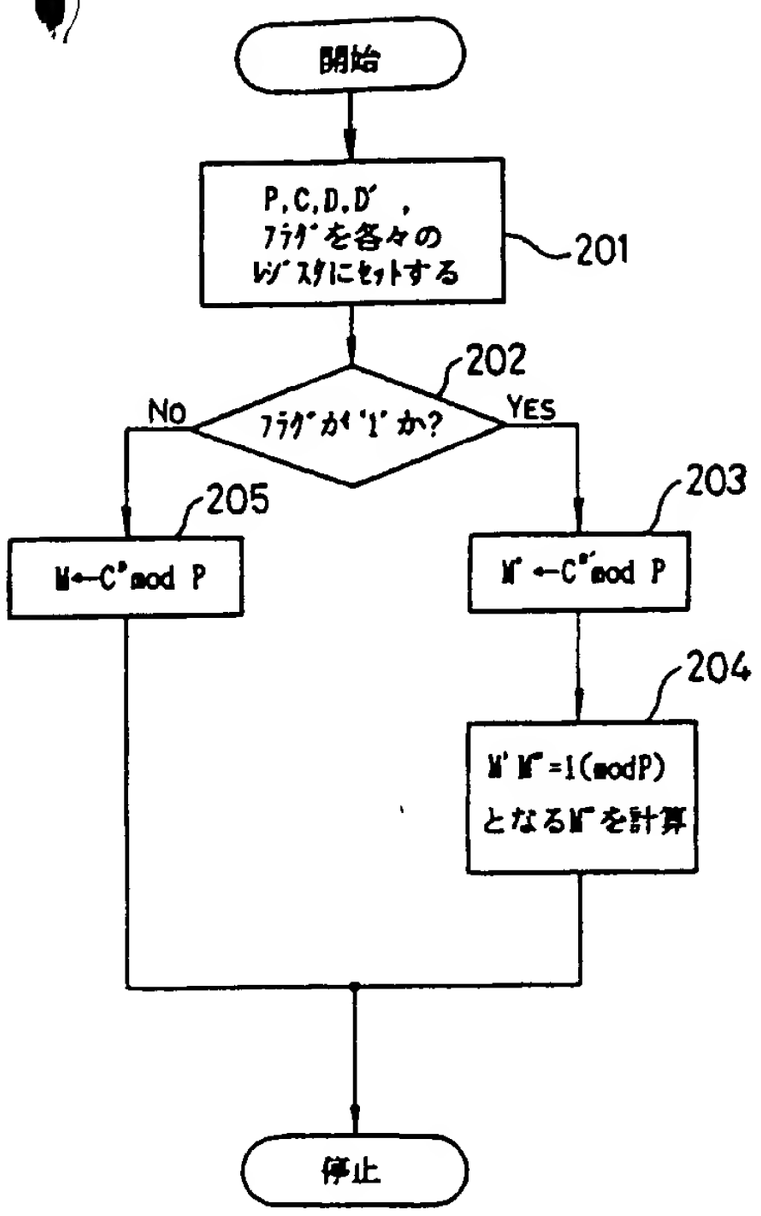
１１０…乗法的逆元計算回路

１１２…Ｄ′を計算する回路

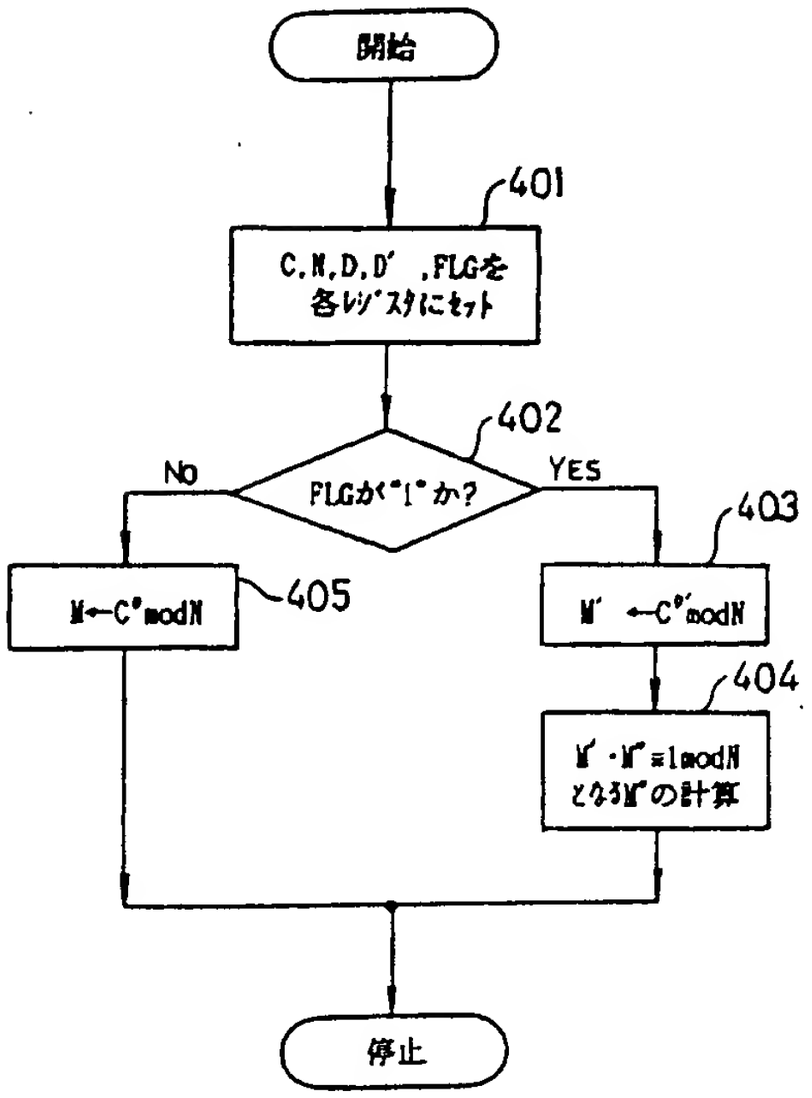
代理人弁理士 三好秀和



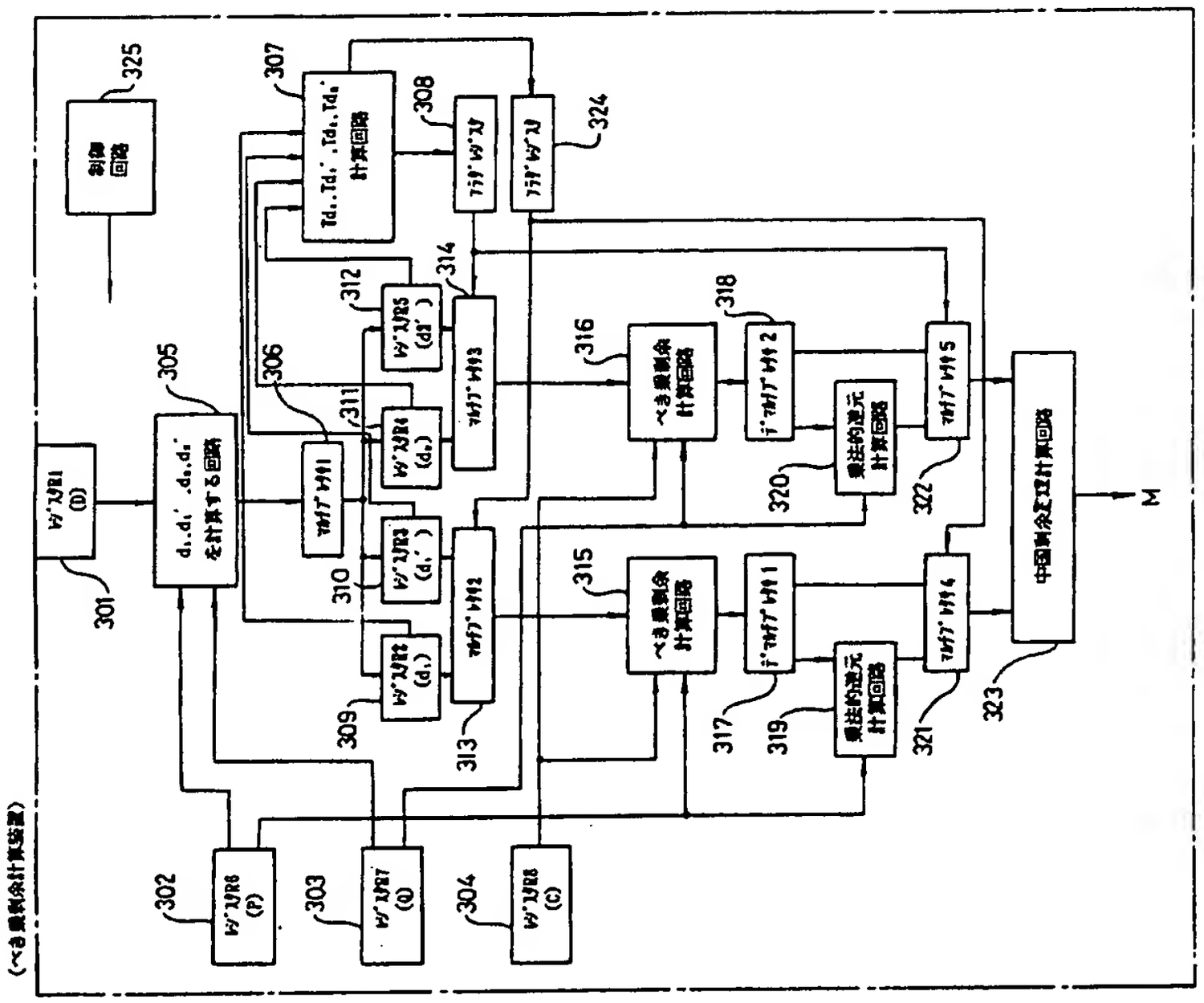
第１図


開始
P,C,D,D′,
フラグを各々の
レジスタにセットする
201
202
フラグが'1'か?
No
YES
205
M←C^D mod P
203
M′←C^D′ mod P
204
M′M″=1(modP)
となるM″を計算
停止

第 2 図


開始
401
C,N,D,D′,FLGを
各レジスタにセット
402
FLGが"1"か?
No
YES
405
M←C^D modN
403
M′←C^D′modN
404
M′・M″≡1modN
となるM″の計算
停止

第 4 図


(べき剰余計算装置)
301
制御回路
305
d1,d1′,d2,d2′
を計算する回路
306
Td1,Td1′,Td2,Td2′
計算回路
307
308
レジスタ
324
レジスタ
311
レジスタ11
312
レジスタ5
(d1′)
314
レジスタ13
316
べき剰余
計算回路
318
レジスタ12
320
乗法的逆元
計算回路
322
レジスタ15
M
310
レジスタ4
(d1)
309
レジスタ3
(d1′)
313
レジスタ14
315
べき剰余
計算回路
317
レジスタ11
319
乗法的逆元
計算回路
321
レジスタ4
323
中国剰余定理計算回路
302
レジスタ6
(P)
303
レジスタ7
(Q)
304
レジスタ8
(C)

第 3 図